



CEH – Ethical Hacking and Countermeasures v11 (e-Learning)

EC-Council

Com certificação

- **Nível:** Intermédio
- **Duração:** -h

Sobre o curso

Certified Ethical Hacker (CEH) é a certificação de ethical hacking mais prestigiada e recomendada pelos empregadores a nível mundial. É a mais desejada certificação em ciber segurança e representa uma das credenciais valorizadas e também exigidas para profissionais que administrem infraestruturas críticas.

Desde o lançamento do CEH em 2003, esta certificação é reconhecida como um padrão dentro da comunidade de segurança da informação. A mais recente versão do CEH v11 continua a apresentar as técnicas de hacking mais recentes e as ferramentas e *exploits* mais avançadas utilizadas por hackers e profissionais de segurança da informação atualmente. As cinco fases de ethical hacking e a missão central original do CEH permanece válida e relevante hoje: ***“To beat a hacker, you need to think like a hacker”***

O CEH v11 cobre mais de 500 novas ameaças e cenários de vulnerabilidade. Incluindo APT, Fileless Malware, Web API Threats, Webhooks, Web Shell, OT Attacks, Cloud Attacks, AI, ML, e muito mais. Os conteúdos estão apenas focados em tecnologias recentes, mas também em tecnologias emergentes, como OT Technology e Container Technology.

Esta nova versão inclui as mais recentes táticas de análise de malware para ransomware, malware bancário e financeiro, botnets IoT, análise de malware OT, malware Android entre outras tais como:

- Incorporating Parrot Security OS
- Re-Mapped to NIST/NICE Framework
- Enhanced Cloud Security, IoT, and OT Modules
 - Cloud-Based Threats
 - IoT Threats
 - Operational Technology (OT) Attacks
- Modern Malware Analysis

- Covering the Latest Threats – Fileless Malware
- New Lab Designs and Operating Systems
- Increased Lab Time and Hands-on Focus
- Industry's Most Comprehensive Tools Library

[Consulte a brochura oficial do curso](#)

Destinatários

Um Certified Ethical Hacker é um especialista que normalmente trabalha num ambiente *red-team*, que está focado em atacar sistemas e obter acesso a redes, aplicações, bases de dados e outros dados críticos em sistemas protegidos. Um CEH compreende as estratégias de ataque, diferentes ângulos de ataque e imita as estratégias de ataque de hackers mal-intencionados. Ao contrário de hackers maliciosos, os Ethical Hackers certificados operam com permissão dos proprietários do sistema e todas as precauções para garantir que os resultados permaneçam confidenciais. *Bug bounty researchers* são especialistas que usam suas competências de ataque para descobrir vulnerabilidades nos sistemas.

Destinatários:

- Information Security Analyst / Administrator
 - Information Assurance (IA) Security Officer
 - Information Security Manager / Specialist
 - Information Systems Security Engineer / Manager
 - Information Security Professionals / Officers
 - Information Security / IT Auditors
 - Risk / Threat / Vulnerability Analyst
 - System Administrators
 - Network Administrators and Engineers
-

Condições

Cursos E-learning EC-Council não beneficiam de isenção de IVA. Ao valor apresentado acresce IVA.

Pré-requisitos

- Experiência em segurança informática
- Fortes conhecimentos práticos de TCP/IP

Metodologia

- Instructor-led, streaming vídeo training modules – Acesso durante 1 ano
- E-courseware oficial (acesso de 1 ano)
- Acesso iLabs – Virtual lab platform – Acesso durante 6 meses
- Manual digital
- Certificado de participação
- Voucher de exame de certificação CEH – *Certified Ethical Hacker v11 exam (312-50)*

Este curso também está disponível no formato Presencial / Live Training.

Para mais informações aceda ao link: [Ethical Hacking and Countermeasures v11 \(CEH\)](#)

Programa

- Introduction to Ethical Hacking
- Footprinting and Reconnaissance
- Scanning Networks
- Enumeration
- Vulnerability Analysis
- System Hacking
- Malware Threats
- Sniffing
- Social Engineering
- Denial-of-Service
- Session Hijacking
- Evading IDS, Firewalls, and Honeypots
- Hacking Web Servers
- Hacking Web Applications
- SQL Injection
- Hacking Wireless Networks
- Hacking Mobile Platforms
- IoT Hacking
- Cloud Computing
- Cryptography